Revised Approach for Smartphone Security Using Cloud and Android Applications

[1]Ms. Diksha Kale, [2]Dr. Sudhir Sawarkar, [3]Prof. Vijay Bhosale

[1]Student of M.E. (Computer), Department of Computer Engineering, MGMCET, Kamothe, Maharashtra, India.
[2] Department of Computer Engineering, DMCE , Airoli, Maharashtra, India
[3] Department of Computer Engineering, MGMCET, Kamothe, Maharashtra, India

Abstract— **Smartphone has emerged as most popular gadget nowadays offering most of functionalities of Personal computer as well as has developing features and applications based on internet, due to which smartphones become vulnerable to security threats similar to the personal computers. Smartphones have limited storage, computational power, processing so implementing intrusion detection and signature based attack detection on smartphone becomes difficult. Cloud computing is a new computing technology gaining attraction in today's world due to its better resource utilization, scalability and cost effectiveness. In this paper we have proposed generic architecture of intrusion detection system for android smartphones as combination of network, cloud and android applications that performs detection of misbehavior within network and able to recover users data from mobile to cloud using an android application. Our system also has another android application that performs intrusion detection on smartphone itself and protects smartphone from malicious download as well as unauthorised access on mobile.**

Keywords—**Android application, Cloud Computing, Intrusion Detection, Malicious files, Misbehavior, Network intrusion, Smartphones.**

I. Introduction

Smartphones have emerged as a type of mobile device providing "all-in-one" convenience by integrating traditional mobile phone functionality and the functionality of handheld computers. Smartphones are also used for web browsing, checking emails ,on-line-banking owing to become target of most of attackers . Enormous numbers of applications are being developed for each of the mobile operating systems (OSs) and each application has its own security requirements (and vulnerabilities). Heterogeneity in hardware, software, and communication protocols to connect to the Internet for all of the different smartphones add complexity when attempting to define security functions for smartphones. Sensitive data such as email and bank passwords are frequently stored by users in an unsafe manner on their smartphones. These poor security practices attract attackers to concentrate on smartphone platforms in order to exploit the vulnerabilities of the smartphone Oss and application software, as well as user generated vulnerabilities. Therefore, there is a growing need to address the security risks associated with smartphones.

The basic security practice for the smartphone is using an antivirus scanning which is resource intensive and affects battery power of the smartphone. In addition to this, antivirus software is based on signature based detection which limits the detection range up to dataset available to that particular software. This dataset again need to update consistently which affects bandwidth efficiency. There are various approaches for intrusion detection of smartphones like network based, host based and cloud based. Cloud based approach based on running multiple detection engines in parallel over cloud and requires full synchronization of mobile phone with replica on cloud which is difficult to achieve. Extra CPU cycles are required to transfer the data for analysis on cloud. Host based approaches directly runs on mobile, these are constrained by mobile phone resources such as battery, storage, processing power.

Most of the approaches focus on detection of misbehaviour by analyzing data which is transferred from mobile to cloud over an encrypted channel. But intrusion prevention and recovery has not been considered in any approach. After detection of misbehaviour, data about misbehaving application, user, and file can be recorded and utilized in further detection of same misbehaviour on the same or other device. This recorded data can be used to trace back the attack source. This important consideration has not been utilized anywhere.

In our project, our aim is to develop an intrusion detection system for android smartphones using network, cloud and android application which will overcome drawbacks of existing approaches and treat intrusion detection and intrusion prevention equally. It should perform intrusion detection within network and recovery of user's important data on smartphone if it detected as an victim. Our system should make use of data obtained during detection (such as corrupt file, misbehaving application etc) for further detection of misbehavior. Our System should prevent user from downloading malicious content from internet as well as user authentication while accessing mobile data and data stored on cloud.

II. LITERATURE SURVEY

A. Paranoid Android Architecture

Portokalidis proposed Paranoid Android which is a cloud based IDS mainly uses record and replay technique. The main invention is to run a synchronized replica of the smartphone in a cloud server. A Tracer records all execution trace of smartphone and then recorded information is forwarded to replayer on cloud over an encrypted channel. Replayer then replays the execution of record on replica of phone. Security checks are performed on the replica. Zero day attacks and memory resident attacks that have targeted mobile phones can be handled. Security functions such as anti-virus, dynamic taint analysis, memory scanners. . Extra CPU cycles are required to send recorded data to replayer [3].

B. Applying Behavioral Detection on Android-Based Devices

A Host-based Intrusion Detection System (HIDS) is realized by behavioral-based framework called Andromaly for Android Smartphone's was presented by Shabtai A. and Elovici Y[6]. Classifying according to their maliciousness and monitoring various features and events on the smartphones, the detection system directly runs on the device .This system is constrained by mobile phone resources such as battery, storage, processing power. The evaluation of their framework is done by testing game and tool application in which the classification algorithm is able to distinguish between those two kinds of applications. The authors evaluate several combinations of classification algorithms and feature selections and conclude that the proposed anomaly detection is feasible on Android devices.

C. Virtualized In-Cloud Security Services for Mobile Devices

Model proposed by Oberheide has a mobile antivirus functionality, moved to a network which works parallel on multiple virtualized malware detection engines [2]. Lightweight mobile host agent and network service are the two main components of this architecture. The former, works on mobile devices, analyses by acquiring files and send them back to the network which is then received by network service that identifies the malicious content. The proposed architecture could be deployed by a mobile service provider or third-party vendor. Mobile devices may enter a disconnected state where the mobile agent may not be able to effectively utilize the network based security services.

D. A cloud based intrusion detection and response system for mobile phones

Houmansadr proposed a cloud-based intrusion detection and response architecture. The architecture emulates a smartphone in the cloud and uses a proxy to duplicate all traffic between the smartphone and the Internet. Intrusion detection on the emulated smartphone is done using resource intense off-the-shelf intrusion forensics and detection systems. To keep the device and the emulated device synchronized, the system replicates the user's input in the cloud [1]. Once misbehavior is detected, the architecture automatically decides upon the best countermeasure, and sends it to the device. A prototype of the forensics engine in the cloud uses a set of intrusion detection systems and the logging of system calls to analyze the installed application.

E. Crowdoid: Behavior based Malware Detection System for Android

Framework for obtaining and analyzing Smartphone application activities called Crowdroid was put forwarded by Burguera [12]. Analysis of the system calls of application on the Smartphone's of many users at a center server by this framework. To differentiate between benign applications and their corresponding malware versions is the main scope of this framework. Applications are not only installed from the internet but also from the official application market there are chances that the copies of malicious application with added malware functionality. Burguera et al. show that their framework is a promising approach to distinguish between a benign application and the corresponding malicious version.

F. Nymble: Blocking Misbehaving Users in Anonymizing Networks

Patrick P. Tsang, Apu Kapadia proposed an approach called Nymble[9]. Users are allowed to access Internet services privately by using Anonymizing networks such as Tor through a series of routers to hide the client's IP address from the server. But some users make abuse of such network anonymity for defacing websites. Website administrator uses IP-address blocking to restrict such misbehaving users but IP-address blocking is not worth when users can use anonymizing networks. Nymble is a system that can blacklist misbehaving users thereby blocking users without their anonymity.

III. PROPOSED SYSTEM

In the proposed system we have an integrated system within network that detects misbehavior within network and with help of an android application fetch victim's data from mobile to cloud to find with whom victim has interacted with in order to prevent further misbehavior. Our system has another android application prevents user from downloading malicious files and unauthorized access on smartphone.

A. Modules of Proposed System

1. Pseudonym manager (PM)

Each user has to register with PM before it connects to internet or particular server of a website.PM assigns each user a unique identifier called Pnym which actually a combination of a random mapping of users identity (suppose IP Address) and MAC [5]. Pnyms are deterministically chosen based on the controlled resource, ensuring that the same Pnym is always issued for the same resource.

2. Nymble manager(NM)

After obtaining Pnym from PM, user connects to Nymble Manager(NM) and requests a nymble (combination of uid, sid) to get an access to particular server .Nymbles are generated using Pnym and server id [5]. These nymbles are thus specific to a particular user-server pair. Nymble manager also checks whether particular user has access to server to which it want to connects. If some user tries to access any file from server unauthorisely then Nymble manager blacklist such user.

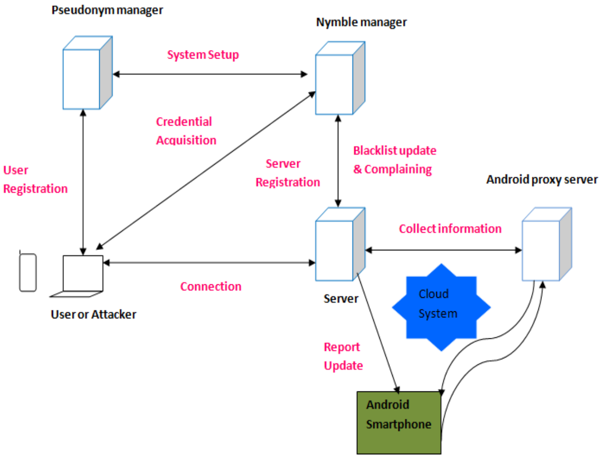


Fig 1: Proposed System Architecture

3. Server

Server maintains list of blacklisted users, generates report of blacklisted users and forward it to android proxy server on cloud.

4. Android Proxy Server

Android Proxy Server is a server on cloud, continuously collecting and updating information about blacklisted users or attackers from Nymble manager and again finding out with which attacker has interacted so that if some user is victim then Android Proxy server has to fetch victims important data from his phone to the cloud for recovery purpose. Using collected data it can find out attacker id, resources used during attack, methods of attack to trace back the attack. Main task of Android Proxy Server is to collect user's important data from his phone and put it on cloud. We have provided user authentication while accessing users data on cloud using OTP generation

5. Android Applications

There are two applications on our smartphone.

Phonesecure is an application on our smartphone that perform recovery of users important data from smartphone. This application is continuously interacting with android proxy server on cloud. Upon receiving a signal from android proxy server, this application collects users data from smartphone and forward it to android proxy server on cloud.

Security is another android application on our phone that perform intrusion detection functionality on mobile itself .By integrating with cloud server this application prevents user from downloading any malicious file to the phone. For that purpose this application uses previously recorded data as well as string matching technique. This application gives a warning message to user before downloading any malicious file and even if user tries to download such file then this application restricts user from download.

IV. HOW THE SYSTEM WORKS?

A. *Nymble Manager System*

1. User registers by entering name, uname, password ,email id, mobile no etc
2. Unique security key generated for each user and mailed to him.
3. User access web page or files on server
4. If user accessing unauthorisely, asked to enter password. If he entered wrong password then he is blocked.
5. Nymble admin checks details of misbehaviour.
6. For further details admin access Phonesecure web service and check details of misbehaving user.

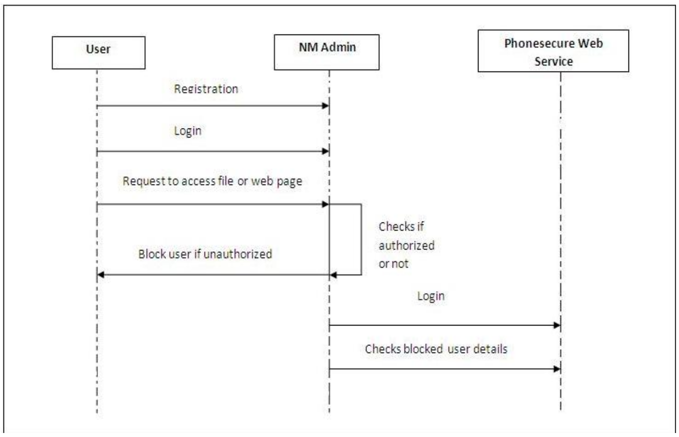

User
NM Admin
Phonesecure Web Service
Registration
Login
Request to access file or web page
Checks if authorized or not
Block user if unauthorized
Login
Checks blocked user details

Fig 2: Message sequence for nymble manager system

B. *Phonesecure Application*

1. New user registers with Phonesecure application
2. Using user id and password and OTP generated on mobile, user logs in Phonesecure web service
3. Through Phonesecure web service user sends message on mobile to recover users data and send it to cloud.
4. Upon receiving message from cloud, phonesecure application collects requested data and pushes it on cloud.

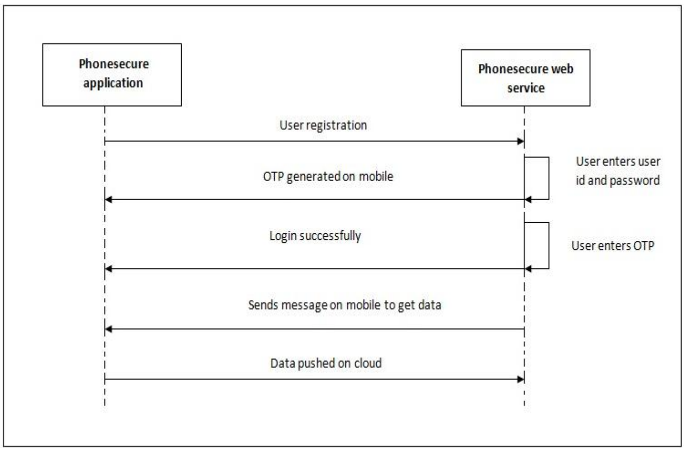


Fig 3: Message sequence for Phonesecure application

C. *Security Application*

1. New user registers with Security application.
2. User logs in security application by entering user id, password followed by security key.

3. If user enters password or security key wrong for three times then he will be blocked for further access.
4. After log in user has three options as upload, download file or application from cloud and check previous log history.
5. If user tries to download any file or application then whether it is malicious or not is detected in two steps
    a. if (file.”ext”==.”ext” of previous malicious files)
        i. then user gets warning that this file extension contain malicious data.
    b. After getting this warning even user attempt to download that file then contents of that file are observed and if it matches with strings in our database then user is restricted to download.
6. There will be list of blocked file in database of our cloud server for which users access will be directly restricted.

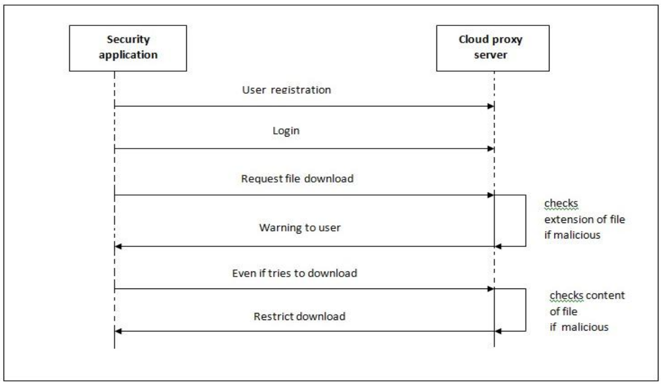


Fig 4: Message sequence for security application

V. RESULTS AND DISCUSSIONS

These are some screenshots obtained during implementation of our system

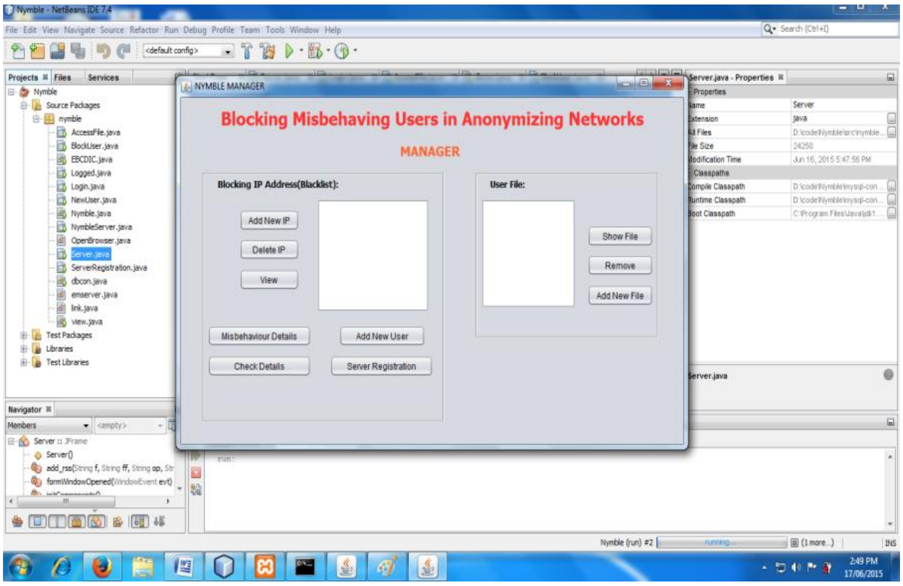
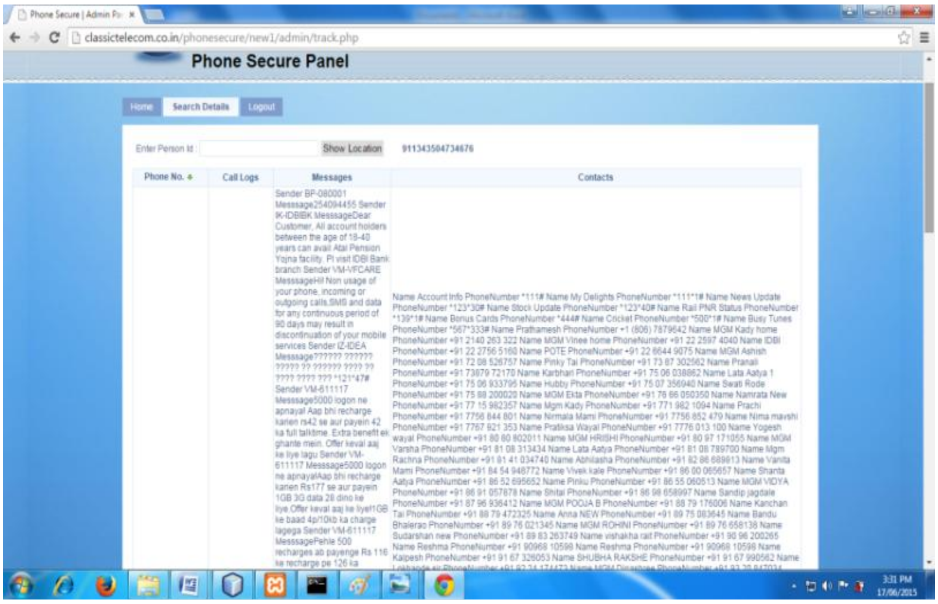


Fig 5:Nymble Manager Admin page

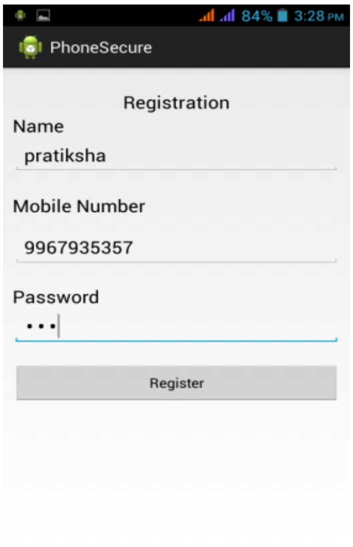


Phone Secure Panel

Enter Person Id : 911343504734676

Phone No.	Call Logs	Messages	Contacts
		Sender BP-080001 Messsage254094455 Sender IK-IDBIBK MesssageDear Customer, All account holders between the age of 18-40 years can avail Atal Pension Yojna facility. Pl visit IDBI Bank branch Sender VM-VFCARE MesssageHi! Non usage of your phone, incoming or outgoing calls,SMS and data for any continuous period of 90 days may result in discontinuation of your mobile services Sender IZ-IDEA Messsage?????? ?????? ????? ?? ?????? ???? ?? ???? ???? ??? *121*47# Sender VM-611117 Messsage5000 logon ne apnaya! Aap bhi recharge karien rs42 se aur payein 42 ka full talktime. Extra benefit ek ghante mein. Offer keval aaj ke liye lagu Sender VM-611117 Messsage5000 logon ne apnaya!Aap bhi recharge karien Rs177 se aur payein 1GB 3G data 28 dino ke liye.Offer keval aaj ke liye!1GB ke baad 4p/10kb ka charge lagega Sender VM-611117 MesssagePehle 500 recharges ab payenge Rs 116 ka recharge pe 126 ka	Name Account Info PhoneNumber *111# Name My Delights PhoneNumber *111*1# Name News Update PhoneNumber *123*30# Name Stock Update PhoneNumber *123*40# Name Rail PNR Status PhoneNumber *139*1# Name Bonus Cards PhoneNumber *444# Name Cricket PhoneNumber *500*1# Name Busy Tunes PhoneNumber *567*333# Name Prathamesh PhoneNumber +1 (806) 7879642 Name MGM Kady home PhoneNumber +91 2140 263 322 Name MGM Vinee home PhoneNumber +91 22 2597 4040 Name IDBI PhoneNumber +91 22 2756 5160 Name POTE PhoneNumber +91 22 6644 9075 Name MGM Ashish PhoneNumber +91 72 08 526757 Name Pinky Tai PhoneNumber +91 73 87 302562 Name Pranali PhoneNumber +91 73879 72170 Name Karbhari PhoneNumber +91 75 06 038862 Name Lata Aatya 1 PhoneNumber +91 75 06 933795 Name Hubby PhoneNumber +91 75 07 356940 Name Swati Rode PhoneNumber +91 75 88 200020 Name MGM Ekta PhoneNumber +91 76 66 050350 Name Namrata New PhoneNumber +91 77 15 982357 Name Mgm Kady PhoneNumber +91 771 982 1094 Name Prachi PhoneNumber +91 7756 844 801 Name Nirmala Mami PhoneNumber +91 7756 852 479 Name Nima mavshi PhoneNumber +91 7767 921 353 Name Pratiksa Wayal PhoneNumber +91 7776 013 100 Name Yogesh wayal PhoneNumber +91 80 80 802011 Name MGM HRISHI PhoneNumber +91 80 97 171055 Name MGM Varsha PhoneNumber +91 81 08 313434 Name Lata Aatya PhoneNumber +91 81 08 789700 Name Mgm Rachna PhoneNumber +91 81 41 034740 Name Abhilasha PhoneNumber +91 82 86 689813 Name Vanita Mami PhoneNumber +91 84 54 948772 Name Vivek kale PhoneNumber +91 86 00 065657 Name Shanta Aatya PhoneNumber +91 86 52 695652 Name Pinku PhoneNumber +91 86 55 060513 Name MGM VIDYA PhoneNumber +91 86 91 057878 Name Shital PhoneNumber +91 86 98 658997 Name Sandip jagdale PhoneNumber +91 87 96 936412 Name MGM POOJA B PhoneNumber +91 88 79 176006 Name Kanchan Tai PhoneNumber +91 88 79 472325 Name Anna NEW PhoneNumber +91 89 75 083645 Name Bandu Bhalerao PhoneNumber +91 89 76 021345 Name MGM ROHINI PhoneNumber +91 89 76 658138 Name Sudarshan new PhoneNumber +91 89 83 263749 Name vishakha rait PhoneNumber +91 90 96 200265 Name Reshma PhoneNumber +91 90968 10598 Name Reshma PhoneNumber +91 90968 10598 Name Kalpesh PhoneNumber +91 91 67 328053 Name SHUBHA RAKSHE PhoneNumber +91 91 67 990562 Name Lokhande sir PhoneNumber +91 92 24 174473 Name MGM Dipashree PhoneNumber +91 93 20 847034

Fig 6 : Misbehaving user details on Phonesecure Web service



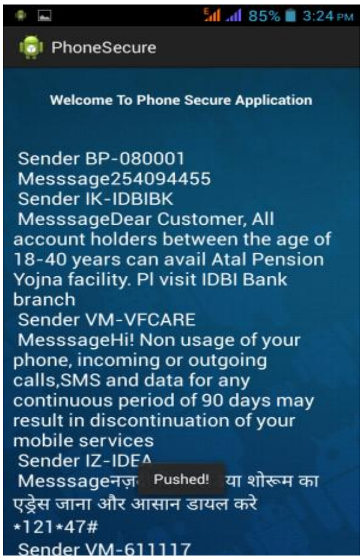
Registration

Name: pratiksha

Mobile Number: 9967935357

Password: •••

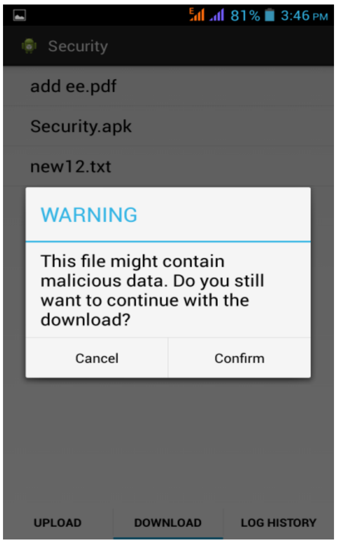
Fig 7: Phonesecure user registration



Welcome To Phone Secure Application

Sender BP-080001
Messsage254094455
Sender IK-IDBIBK
MesssageDear Customer, All account holders between the age of 18-40 years can avail Atal Pension Yojna facility. Pl visit IDBI Bank branch
Sender VM-VFCARE
MesssageHi! Non usage of your phone, incoming or outgoing calls,SMS and data for any continuous period of 90 days may result in discontinuation of your mobile services
Sender IZ-IDEA
Messsageनज़ या शोरूम का एड्रेस जाना और आसान डायल करे *121*47#
Sender VM-611117

Fig 8:Phonesecure Application pushing data on cloud



add ee.pdf

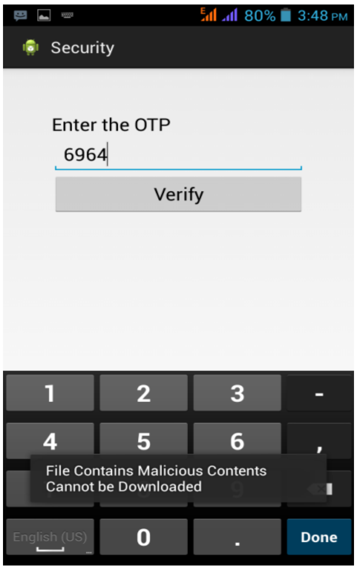
Security.apk

new12.txt

WARNING

This file might contain malicious data. Do you still want to continue with the download?

Fig 9 : Warning before malicious download



Enter the OTP: 6964

File Contains Malicious Contents Cannot be Downloaded

Fig 10 : Malicious download restricted

As we have seen resource utilization is an important **f**actor for intrusion detection system for android smartphones. Here we have observed CPU, memory and battery usage of our intrusion detection, recovery systems applications on smartphone. For this observation we have chosen Micromax A114 android 4.2 device with technical specifications as below

CPU Processing speed	1.3GHz quad core
Memory	RAM - 1GB , ROM - 4GB
Battery	Li-ion battery with 2000mAh capacity

Table 1: Specification of Smartphone

Battery monitor widget and System panel task manager are used for measurement of battery utilization and memory, CPU utilization respectively. For any random instance of time we run our Phonesecure and security applications and we have obtained following observations.

Resources/applications	Security	Phonesecure
CPU	4.0%	3.9%
Memory	2.37%	1.51%
Battery	2.3%	6.2%

Table 2: Resource Utilization

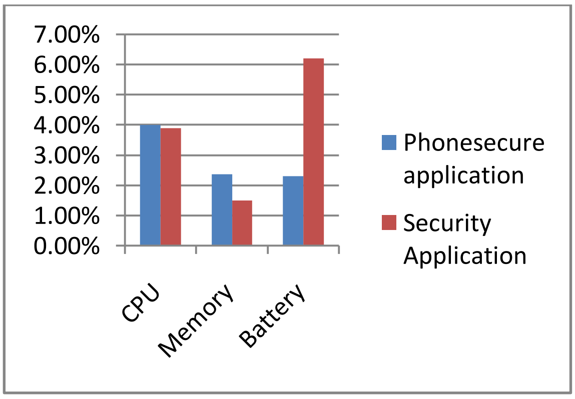


Fig.11: Performance of Proposed system in terms of Resource utilization

From the above chart we get to know that our proposed systems applications that are security and Phonesecure consumes very less amount of resources i.e. CPU, memory and battery capacity as compared to antivirus functionality used in previous approaches as well as resources used for synchronization of replica with smartphone.

VI. CONCLUSION AND FUTURE SCOPE

Our system is a new approach of intrusion detection, prevention and recovery for android smartphones with limited resources. System identifies intrusion detection within network and recovers data from smartphone to cloud for any user identified as victim. If user tries to download any unsecured file or application, system detects such intrusion and produces accurate response so that user can think twice while downloading such file or application. Even if user tries to download such malicious file then user is restricted for that activity. Our system can block misbehaving users and applications. Our system provides user authentication for accessing user's data on cloud and downloading files from cloud server.

Future scope of work done is to explore different detection methods in android application so that variations in misbehavior of user or application can be detected. Application performing recovery must be improved in a way to choose appropriate recovery option.

REFERENCES

[1] Amir Houmansadr, Saman A. Zonouz, and Robin Berthier. A cloud-based intrusion detection and response system for mobile phones. In Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and NetworksWorkshops, DSNW '11, pages 31–32, Washington, DC, USA, 2011. IEEE Computer Society

[2] Jon Oberheide, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn, and Farnam Jahanian. Virtualized In-Cloud Security Services for Mobile Devices. In Workshop on Virtualization in Mobile Computing (MobiVirt '08), Breckenridge, Colorado, June2008

[3] Georgios Portokalidis, Philip Homburg, Kostas Anagnostakis, and Herbert Bos. Paranoid android: versatile protection for smartphones. In Proceedings of the 26th Annual Computer Security Applications Conference, 2010

[4] Philipp Stephanow Lakshmi Subramanian, Gerald Q. Maguire Jr. An architecture to provide cloud based security services for smartphones, 2011.

[5] Rohit S. Khune and J. Thangakumar. A Cloud-Based Intrusion Detection System for Android Smartphones. 2012 International Conference on Radar, Communication and Computing.

[6] Asaf Shabtai and Yuval Elovici. Applying behavioral detection on android-based devices. In MOBILWARE, pages 235–249, 2010.

[7] Rasnam Kaur, Amardeep Kaur. Analysis Of Behaviour Of Security As A Service In Cloud For Smartphones. International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012 ISSN: 2278-0181

[8] Lakshmi Subramanian, Gerald Q. Maguire Jr., Philipp Stephanow. An Architecture To Provide Cloud Based Security Services For Smartphones

[9] Patrick P. Tsang, Apu Kapadia, Member, IEEE, Cory Cornelius, and Sean W. Smith Nymble: Blocking Misbehaving Users in Anonymizing Networks.

[10] Anand Joshi, Arshiya Shaikh, Aruna Kadam , Vasudha Sahu. NYMBLE BLOCKING SYSTEM. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.2, April 2012

[11] Kenji Morita, Platform for Pushing the Device-Oriented Information into a Cloud. Department of Advanced Information Technology, Graduate School of Information Science and Electrical Engineering Kyushu University 744 Motooka Nishi-ku, Fukuoka 819-0395, Japan.

[12] Iker Burguera, Urko Zurutuza, and Simin N. Tehrani. Crowdroid: behavior-based malware detection system for Android. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, SPSM '11, pages 15–26, New York, NY, USA, October 2011. ACM.

[13] Mr. Vishal S. Patil, Mr. Chetan J. Shelke. Revisiting Defense against Malwares in Android using Cloud Services. International Journal of Application or Innovation in Engineering & Management (IJAIEM). Volume 3, Issue 3, March 2014 ISSN 2319 – 4847

[14] Namitha Jacob. Intrusion Detection in Cloud for Smart Phones. International Journal of Research in Engineering & Advanced Technology (IJREAT), Volume 1, Issue 1, March, 2013 ISSN: 2320 – 8791

[15] Hatem Hamad, Mahmoud Al-Hoby. Managing Intrusion Detection as a Service in Cloud Networks. International Journal of Computer Applications (0975 – 8887) Volume 41– No.1, March 2012.

[16] Oyeleye Christopher A. , Daramola Comfort Y., Akinpelu James A. Mob-AIDS: An Intrusion Detection System for the Android Mobile Enterprise. IJCSI International Journal of Computer Science Issues, Vol. 11, Issue 3, No 2, May 2014

[17] Suhas Holla, Mahima M Katti ANDROID BASED MOBILE APPLICATION DEVELOPMENT and its SECURITY.International Journal of Computer Trends and Technology- volume3Issue3- 2012

[18] Ria Das Indrajit Das. Smartphone Security by Cloud Computing. International Journal of Innovations in Engineering and Technology (IJIET) Vol. 2 Issue 3 June 2013 ISSN: 2319-1058.